Cassandra Crossing/ Tor, lezioni di server 5

(100)—L'installazione del router Tor è ora a portata di mano, con pochi piccoli passi: Marco Calamari con la nuova lezione spiega come…

Cassandra Crossing/ Tor, lezioni di server 5

Figure 1:

(100)—L'installazione del router Tor è ora a portata di mano, con pochi piccoli passi: Marco Calamari con la nuova lezione spiega come attivare il sospirato strumento di tutela e difesa della privacy. Ecco cosa fare.

16 novembre 2007—La scorsa settimana molte persone si sono fatte un'idea più precisa di cosa è un router Tor e di cosa significa decidere di crearne uno, sia dal punto di vista filosofico e morale, sia da quello legale. Prima di proseguire parlando di tecnica, è necessaria una precisazione che penso risponderà ad alcuni dubbi espressi sul forum della settimana scorsa.

Per quanto riguarda l'ampia esperienza del nostro gruppo e degli amministratori di router Tor con cui siamo in contatto, l'unica tipologia di interazione avvenuta con indagini di polizia in Italia è stata quella descritta nella scorsa rubrica.

Questo non può ovviamente escludere che siano avvenute, o possano avvenire, altri tipi di interazioni, come ad esempio perquisizioni e sequestri di materiale informatico che la magistratura ha l'autorità di far eseguire quando ritenga che possano sussistere ipotesi di reato.

Per quanto ci è noto, negli ultimi due anni c'è stato un unico caso, avvenuto in Germania, in cui almeno 3 operatori sono stati oggetto di perquisizioni nell'ambito di una stessa indagine che pare riguardasse (non è nemmeno il caso di dirlo) una questione di pedopornografia, e che non ha portato nessuna imputazione e tantomeno condanna degli operatori Tor coinvolti.

Nello stesso periodo, come tutti sappiamo, ci sono state invece migliaia di perquisizioni e di sequestri di materiale informatico legate a semplici scambi di mail rilevanti per indagini di polizia, a copia di materiale protetto da copyright e per utilizzo illegale di reti peer-to-peer.

E' comunque senz'altro vero che esistono passatempi decisamente più tranquilli che gestire un router Tor, come ad esempio collezionare etichette di vino, o farsi semplicemente e su scala industriale gli affari propri e basta.

Ma rientriamo in tema; alcune persone, sperabilmente molte, avranno preso in considerazione l'impresa di realizzare un router Tor, e sono perciò in attesa di questa puntata; altre magari avranno preso la palla al balzo e, valendosi delle ottime istruzioni sia per Windows che per Linux, reperibili sul sito Tor di EFF, si sono già messe all'opera.

Quasi tutti avranno notato che lavoro abitualmente solo su Linux, e che dove necessario descrivo le applicazioni in ambiente Windows "per differenza".

Con gioia degli utenti con solo "finestre", oggi invertirò il mio punto di vista, descrivendo l'installazione di un router Tor in ambiente Windows. Questa scelta non è dovuta solo al numero degli utenti Redmond-centrici, ma soprattutto alla disponibilità di un bundle (un gruppo di programmi, che si configura praticamente da solo come client, ed in maniera elementare come server).

Gli utenti *nix e GNU/Linux d'altra parte sono abbastanza smaliziati per poter seguire queste semplicissime istruzioni, e se specialmente usano Debian sono distanti solo un paio di apt-get dal risultato.

Poche volte in vita mia mi sono trovato di fronte ad un'applicazione server cosi bene integrata e leggera come il bundle Tor/Privoxy/Vidalia/TorButton scaricabile da questa pagina.

L'installazione e l'avvio sono indolori; è pero' d'obbligo ricordare che dovete trovarvi su un'ADSL flat, con un IP pubblico e che non sia filtrata. Servono infatti due porte TCP, di solito 9001 e 9030 (ma si possono cambiare) raggiungibili da Internet.

Tor è comunque in grado di verificarlo da solo, come potete vedere facendo attenzione ai messaggi di log quando farete partire il vostro nodo come server. Per renderle raggiungibili è necessario anche avere un nome host pubblico, ma questo non è un problema.

Bastano infatti pochi minuti per registrare gratuitamente il vostro su uno dei tanti provider come ad esempio DynDNS ed installare il client dyndns che "battezzerà" l'indirizzo ip dinamico del vostro PC con un nome a vostra scelta. Vi ricordo che la lista e-privacy è come sempre a disposizione per indicazioni e chiarimenti.

Appena terminata l'installazione, eseguita selezionando la lingua italiana (caso raro ma piacevole) Tor, Privoxy e Vidalia partiranno automaticamente e vi si presenterà la finestra del pannello di controllo di Vidalia, che permette di gestire anche Tor. Aprite le finestre dei log, della mappa e della banda, lanciate il vostro Firefox, ben configurato nelle precedenti lezioni (non vorrete mica usare Internet Explorer, vero?) e vi troverete davanti ad un desktop come questo:
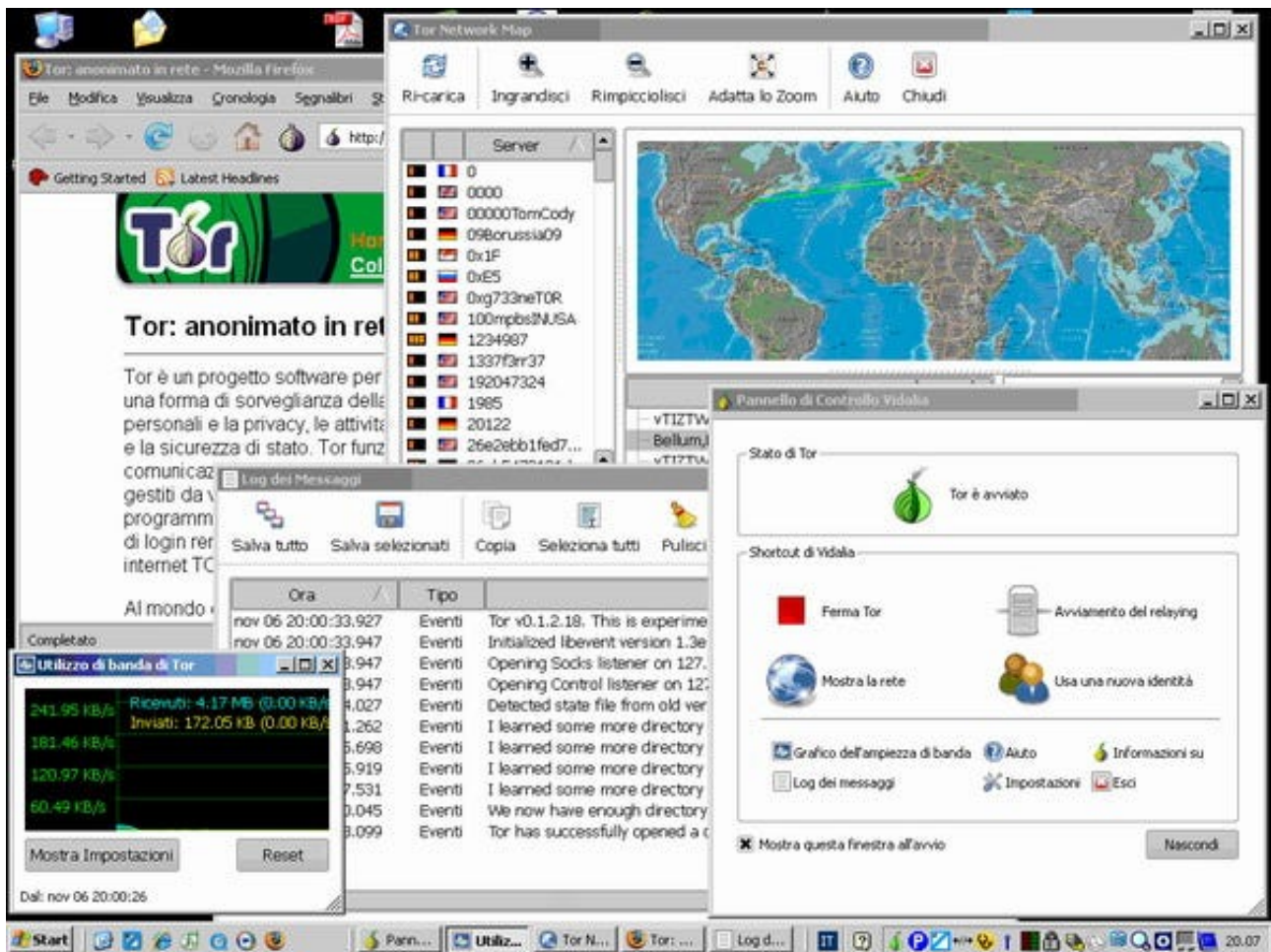
Figure 2:

Prima di proseguire, abbiate cura di controllare che sia possibile raggiungere Internet sia normalmente che attraverso la rete Tor, collegandovi all'oramai notissimo Torcheck e cambiando stato utilizzando il pulsante di TorButton.

Ponete un occhio ai messaggi di log che scorrono durante la navigazione e seguite l'apertura e la chiusura delle connessioni utilizzando la mappa zoomabile. Per vedere sulla mappa la rappresentazione di uno dei quattro circuiti che in ogni momento Tor tiene aperti per voi e che sono elencati sotto la mappa, vi basterà selezionarli con il mouse.

Allora ci siamo; attiviamo l'iperguida e diventiamo server. Nel pannello di controllo di Vidalia:
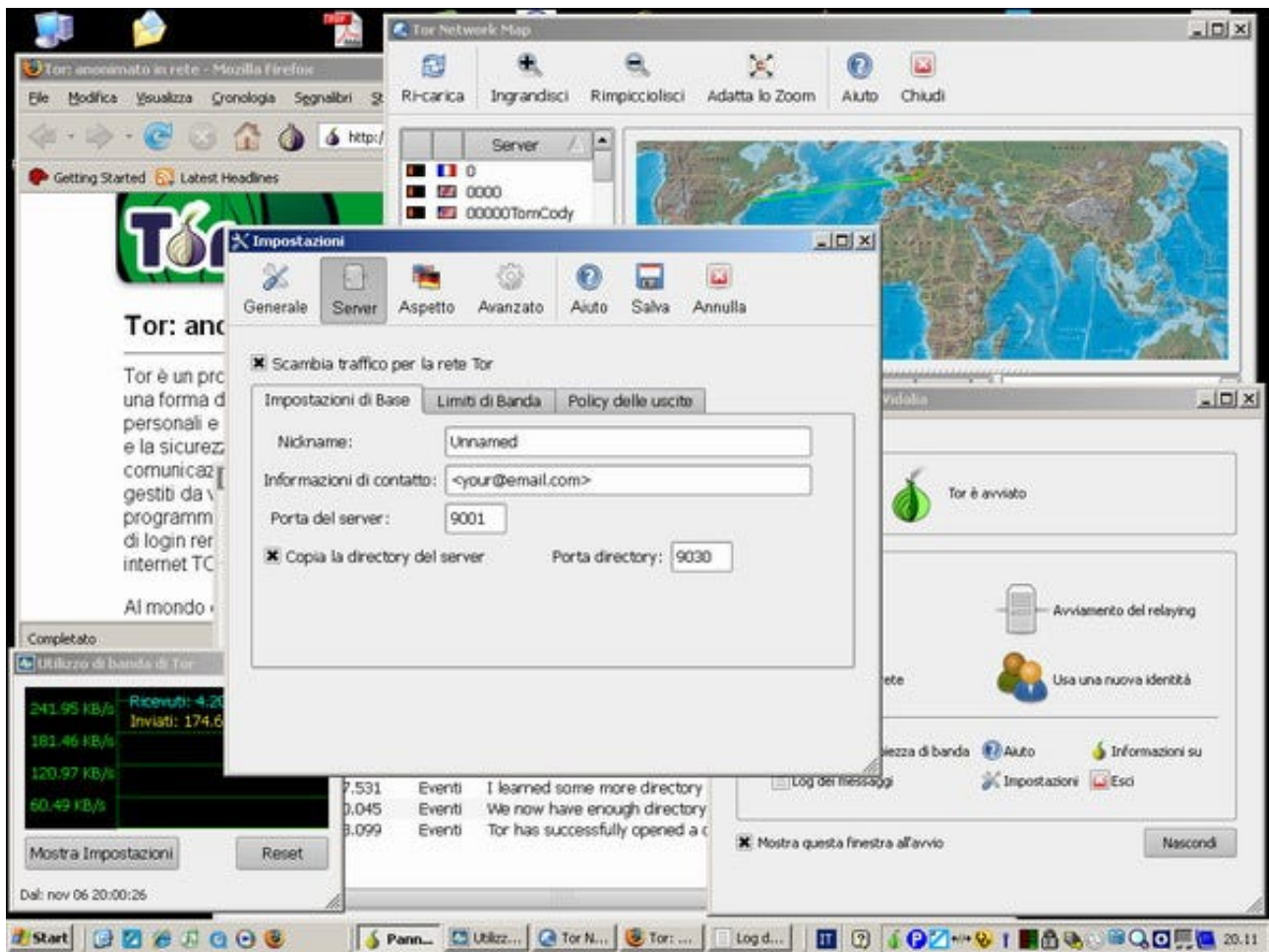
Figure 3:

Cliccate sull'icona Server e spuntate l'anonima casellina "Scambia traffico per la rete Tor" che vi si presenterà. Inserite un nickname per il vostro server ed un indirizzo di posta per contatti amministrativi (ambedue facoltativi). Non spuntate per adesso la casella "Copia la directory del server"; vedremo poi perché.
Andate ora sulla linguetta "Limiti di banda":
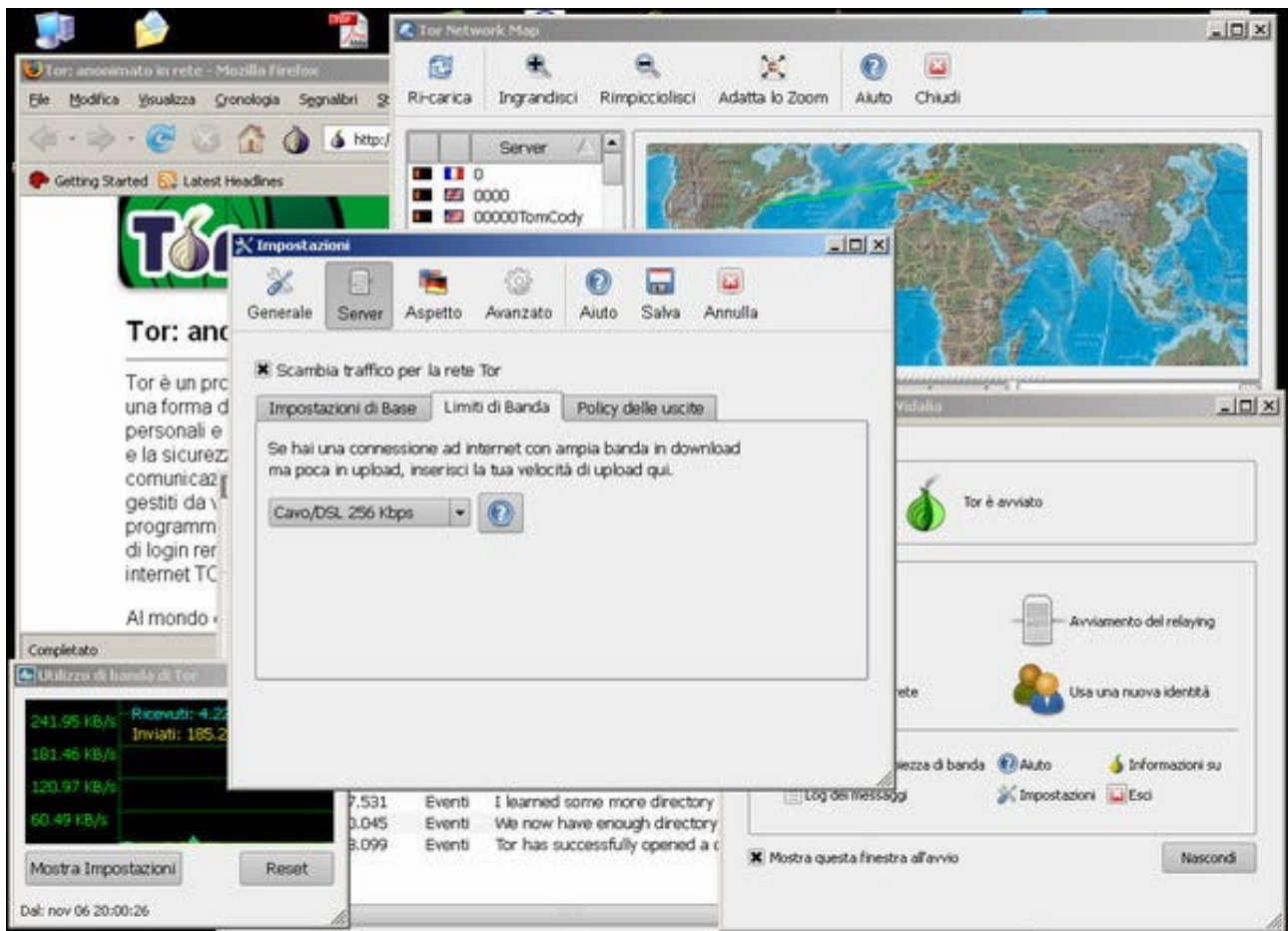
Figure 4:

e selezionate il valore 256K. Non preoccupatevi per la vostra banda, è un valore di picco che non viene mai raggiunto. In ogni caso, se notaste prolungati rallentamenti potete diminuirlo, avendo cura di non scendere sottoi i 150K.

Infine, giusto per volare un po' più bassi, selezionate la linguetta "Policy delle uscite"
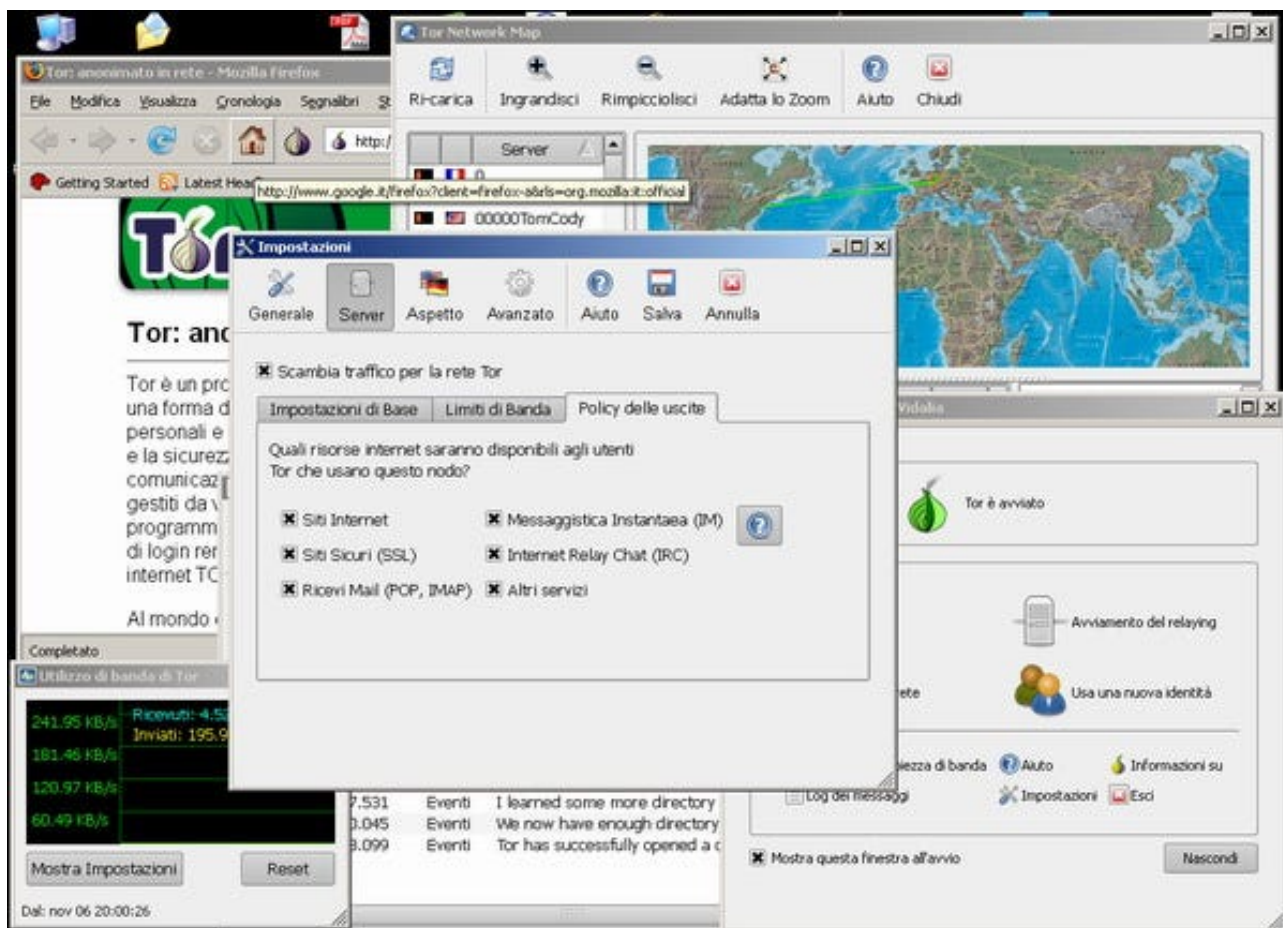
Figure 5:

e togliete il segno di spunta da "altri servizi". Anche su questo torneremo prossimamente. Un click sull'icona Salva ed abbiamo finito.

Contrariamente a quella del Millennium Falcon, se l'Impero non vi ha nel frattempo intercettato filtrato, la vostra iperguida sarà in piena attività, ed il vostro router Tor starà fornendo privacy a centinaia di navigatori.

Ora è il momento di leggersi religiosamente tutta l'ottima documentazione italiana presente sul sito e se necessario chiedere lumi ad amministratori navigati. Nella prossima puntata un po' di dettagli e di tuning.

Buon lavoro.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on August 30, 2023.

Canonical link

Exported from Medium on August 27, 2025.